The Modes of Recovery of Stolen Cryptocurrency Assets in Singapore

Written by

Ng Yuan Siang, Practice Trainee
e: yuansiang@thuraisingam.com

Edited by

Chooi Jing Yen, Partner
e: jingyen@thuraisingam.com

I. Introduction

1 On 1 November 2008, the pseudonymous Satoshi Nakamoto published a white paper on a trust-less, peer-to-peer electronic cash system based on cryptographic proof, with every transaction stored on a decentralised 'blockchain'.[1] The Bitcoin network soon sparked an upheaval of the global financial system a little more than a decade later. Cryptocurrencies like Bitcoin have come to be accepted as credible financial assets. Institutions have poured their money into cryptocurrencies, with the global market capitalisation of all cryptocurrencies hovering at more than US$1 trillion as of May 2022,[2] while El Salvador has become the first country to accept BTC as legal tender.[3]

2 The law has been left playing catch-up with the paradigm shifts that cryptocurrencies and blockchain technology have brought along with them. Unsavoury characters like hackers, money launderers and scammers have nestled comfortably within the murky contours of crypto. Yet when it comes to pursuing justice against these bad actors, one must first deal with fundamental questions – are cryptocurrencies even property? Can an injunction be

[1] Nakamoto, S. (1 November, 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Retrieved from https://bitcoin.org/bitcoin.pdf.
[2] CoinMarketCap. (19 May, 2022). *Global Cryptocurrency Charts*. Retrieved from CoinMarketCap: https://coinmarketcap.com/charts/.
[3] Renteria, N. (25 June, 2021). *Bitcoin to become legal tender in El Salvador on Sept 7*. Retrieved from Reuters: https://www.reuters.com/technology/bitcoin-become-legal-tender-el-salvador-sept-7-2021-06-25/

ordered against a crypto wallet? Even if an injunction can be ordered, how would one enforce it? This article discusses how the Singapore court has dealt with some of the issues, and analyses the potential challenges ahead.

II. *Mareva* and proprietary injunctions – the present position in Singapore

3 In Singapore, the recent decision in *CLM v CLN* [2022] SGHC 46 ("*CLM*") is a good springboard to discuss how stolen cryptocurrency assets have been dealt with. We summarise the brief facts and salient points of the judgment before analysing the implications of *CLM*.

(1) *Dramatis personae*

4 *CLM* involves eight distinct anonymous parties. For convenience and readability, we lay out descriptions of each of the parties as well as their role in respect of *CLM*:-

(a) CLM ("**the Plaintiff**"), the plaintiff in Suit No 470 of 2021 ("**Suit 470**"), is an American national and entrepreneur who claims to have had 109.83 Bitcoin ("**BTC**") and 1497.54 Ether ("**ETH**") (collectively, the "**Stolen Cryptocurrency Assets**") stolen from him by unknown individuals;
(b) CLN ("**the First Defendants**") are persons unknown, and is essentially a placeholder representing any person or entity who carried out, participated in or assisted in the theft of the Stolen Cryptocurrency Assets;
(c) CLO ("**the Second Defendant**") is an entity incorporated in the Cayman Islands and runs a centralised cryptocurrency exchange ("CEX")[4] with operations in Singapore;
(d) CLP ("**the Third Defendant**") is an entity incorporated in Seychelles and also runs a CEX with operations in Singapore;
(e) CPZ and CQA (the "**Fourth Defendant**" and "**Fifth Defendant**" respectively), are foreign nationals within the First Defendants; in other words, they are two known individuals who were identified to have carried out, participated in or assisted in the theft of the Stolen Cryptocurrency Assets;
(f) CQB ("**the Sixth Defendant**") is an entity incorporated in the United States and runs a CEX with operations in Singapore;
(g) CQC ("**the Seventh Defendant**") is an entity incorporated in the United States which provides financial and digital payment services, with operations in Singapore.[5]

(2) *A primer on digital wallets and cryptocurrency-related concepts*

5 The Bitcoin and Ethereum networks are peer-to-peer payment networks where parties can transact with each other without the need for a trusted middleman,

[4] As opposed to a decentralised cryptocurrency exchange, though the distinction is inconsequential for present purposes.
[5] *CLM v CLN* [2022] SGHC 46 at [2], [6], [7], [8], [61], [62] and [66].

such as a bank, to validate transactions. Instead, validation is done by a network of computers around the world connected to a **blockchain**, a decentralised record of every cryptocurrency transaction on the network. Each cryptocurrency network generally has its own blockchain. On the Bitcoin and Ethereum networks, all transactions and account balances are fully transparent and accessible by anyone on the Internet.[6]

6 To access a cryptocurrency network, one needs a **digital wallet**. Every digital wallet has its own **public** and **private key**. They are analogous, respectively, to an email address and password. Transactions are addressed to and received from one public key to another, much like how emails are sent and received from one email address to another.[7]

7 Since a private key may consist of up to 256 random characters, they are usually translated into a randomly generated **seed phrase** of 12 or 24 English words, which is essentially like a password. Being in possession of this seed phrase grants you access to the private key of the associated digital wallet, which in turn gives you full control of said wallet, including the ability to empty it of all its contents.[8] Given the dire consequences of losing one's seed phrase, some choose to keep it in places far from the reaches of the Internet. For example, one may write their seed phrase on a piece of paper and store it in a safe deposit box. The Plaintiff himself stored his seed phrase in a safe in his apartment in Mexico.[9]

8 Digital wallets may be separated into two broad categories, **non-custodial wallets** and **custodial wallets**. Non-custodial wallets are essentially wallets that belong fully to the user, who has control over its seed phrase and consequently its private key. The Exodus and BRD wallets[10] used by the Plaintiff belong to this category. Custodial wallets are typically, though not exclusively, associated with CEXs. When a customer wishes to send cryptocurrency to a CEX to make use of its services, one generally addresses the transaction to a digital wallet that the CEX has custody over.[11] Customers essentially "deposit" their cryptocurrencies into the CEX's wallets, similar to how one deposits money into a bank. CEXs then attribute incoming transactions to customers' accounts internally on their own records. These internal allocations are not reflected on the blockchain itself – on the blockchain, all an outsider would see is that some cryptocurrency was deposited into a wallet

[6] All that is required is a blockchain explorer, such as blockchain.com/explorer?view=btc for the Bitcoin network and etherscan.io for the Ethereum network.
[7] *CLM v CLN* [2022] SGHC 46 at [10].
[8] Nibley, B. (2 November, 2021). *What is a Bitcoin Seed Phrase? Seeds vs. Private Keys*. Retrieved from SoFi: https://www.sofi.com/learn/content/what-is-a-bitcoin-seed-phrase/.
[9] *CLM v CLN* [2022] SGHC 46 at [17].
[10] *CLM v CLN* [2022] SGHC 46 at [15].
[11] In other words, a digital wallet that *only* the CEX has the private key to.

belonging to the CEX.[12]

(3) *Brief facts*

9 The Plaintiff commenced Suit 470 after the seed phrases to two of his non-custodial wallets were stolen from his safe in Mexico. Using those seed phrases, the First Defendants drained the Plaintiff's wallets, funnelling the Stolen Cryptocurrency Assets to a series of digital wallets. Some of the Stolen Cryptocurrency Assets eventually found its way to custodial wallets that were identified to belong to the Second and Third Defendants.[13]

10 *CLM* itself concerned two separate *ex parte* applications brought by the Plaintiff.

(4) *Summons No 2444 of 2021 ("**SUM 2444**")*

11 The first application, SUM 2444, was an *ex parte* application for a proprietary injunction and worldwide *Mareva* injunction prohibiting the First Defendants from dealing with, disposing of, or diminishing the value of the Stolen Cryptocurrency Assets, as well as for ancillary disclosure orders against the Second and Third Defendants to assist in tracing the Stolen Cryptocurrency Assets and identifying the First Defendants.[14]

12 The Honourable Lee Seiu Kin J first considered the question of whether the General Division of the High Court ("**the Court**") had jurisdiction over unknown persons. He answered this question in the affirmative, though he added the caveat that the description of such unknown persons must be sufficiently certain as to identify those who are included and those who are not. He found that the present description of the First Defendants was sufficiently certain.[15]

13 The Court then went on to consider whether a proprietary injunction should be granted to prohibit the First Defendants from dealing with, disposing of or diminishing the value of the Stolen Cryptocurrency Assets. The following principles, as laid out in *Bouvier, Yves Charles Edgar and another v Accent Delight International Ltd and another and another appeal* [2015] 5 SLR 558, were applicable:-

(a) There must have been a serious issue to be tried; and

(b) The balance of convenience must have laid in favour of granting the injunction. [16]

14 First, the Court found that the main question was whether the Stolen Cryptocurrency Assets were capable of giving rise to proprietary rights that could be protected via a proprietary injunction. Given that this was an interlocutory

[12] Bitcoin.com. (n.d.). *What's a non-custodial wallet?* Retrieved from https://www.bitcoin.com/get-started/custodial-non-custodial-bitcoin-wallets/.
[13] *CLM v CLN* [2022] SGHC 46 at [17]-[21].
[14] *CLM v CLN* [2022] SGHC 46 at [3].
[15] *CLM v CLN* [2022] SGHC 46 at [23]-[35].
[16] *CLM v CLN* [2022] SGHC 46 at [36]-[38].

application in which the Plaintiff need only show a serious arguable case, the Court did not consider this issue in detail. Reading the four requirements in the definition of a property right laid out in *National Provincial Bank Ltd v Ainsworth* [1965] AC 1175 ("*Ainsworth*") with *Ruscoe v Cryptopia Ltd (in liq)* [2020] 2 NZLR 809, the Court found that cryptocurrencies satisfied the *Ainsworth* definition of a property right, and the Plaintiff was therefore able to prove that he had a serious issue to be tried.[17]

15 Second, the Court also found that the balance of convenience lay in the favour of granting the injunction given the real risk that the First Defendants would dissipate the Stolen Cryptocurrency Assets.[18]

16 The proprietary injunction was therefore granted.[19]

17 As for the worldwide *Mareva* injunction, the Court found that the requirement for a good arguable case on the merits of the claim was easily satisfied, because the law, when applied on the facts, would clearly give rise to the claims sought by the Plaintiff.[20]

18 The Court also found that there was a real risk of dissipation. The First Defendants had already been dissipating the Stolen Cryptocurrency Assets. The Court also noted that the nature of cryptocurrency made it easy to further dissipate and hide cryptocurrencies in cyberspace.[21]

19 Agreeing with the Plaintiff that the First Defendants were unlikely to have sufficient assets in Singapore to satisfy an award of damages, the Court granted the worldwide *Mareva* injunction.[22]

20 The Court also granted the ancillary disclosure orders against the Second and Third Defendants.[23]

(5) *Summons No 4880 of 2021 ("**SUM 4800**")*

21 The second application, SUM 4800, came sometime after the reliefs sought in SUM 2444 were granted by the Court. The Second and Third Defendants complied with the ancillary disclosure orders in SUM 2444, which allowed the Plaintiff to identify the Fourth and Fifth Defendants, two individuals who had used the Second and Third Defendants' CEX services to deal with the Stolen Cryptocurrency Assets. They also found that the Fourth and Fifth Defendants had transferred part of the

[17] *CLM v CLN* [2022] SGHC 46 at [39]-[46].
[18] *CLM v CLN* [2022] SGHC 46 at [47]-[48].
[19] *CLM v CLN* [2022] SGHC 46 at [49].
[20] *CLM v CLN* [2022] SGHC 46 at [53].
[21] *CLM v CLN* [2022] SGHC 46 at [54].
[22] *CLM v CLN* [2022] SGHC 46 at [55]-[56].
[23] *CLM v CLN* [2022] SGHC 46 at [57]-[60].

Stolen Cryptocurrency Assets to custodial wallets belonging to the Sixth and Seventh Defendants.[24]

22 SUM 4800 was therefore an application for leave to serve the Fourth and Fifth Defendants out of jurisdiction by substituted means, as well as to join the Fourth to Seventh Defendants to Suit 470.[25] All the applications in SUM 4800 were granted, save for some minor corrections as to phrasing.[26]

III. Implications of the decision in *CLM*

23 After *CLM*, it seems to be accepted that property rights may subsist in cryptocurrency assets, and that the Singapore Courts have the power to award interlocutory reliefs such as proprietary and *Mareva* injunctions against such assets. Two months after *CLM*, the Court granted another landmark injunction to stop the potential sale and transfer of a misappropriated rare non-fungible token ("**NFT**"), BAYC#2162.[27]

24 However, the decision in *CLM* should be seen with a few caveats.

25 **First**, it should be noted that the finding in *CLM* that cryptocurrency assets are capable of giving rise to proprietary rights was not arrived at after a full trial. Since only injunctive reliefs were sought, the Plaintiff only needed to show a serious arguable case that the Stolen Cryptocurrency Assets could be the subject of an injunction.[28] The Court did not engage in complex questions of law or fact when arriving at its conclusion.[29] There remains, however slim, a possibility that another court may arrive at a different conclusion after comprehensively considering the issue.

26 **Second**, even if proprietary and *Mareva* injunctions come to be well-accepted as potential remedies for misappropriated cryptocurrency assets, they are by no means a panacea. Unlike financial assets in banks, which can swiftly become subject to injunctions once the banks are notified, the enforcement and effectiveness of injunctive reliefs against cryptocurrencies heavily depends on the facts of every case.

27 Proprietary and *Mareva* injunctions were appropriate in *CLM* because of its specific facts and the manner in which the First Defendants misappropriated the Stolen Cryptocurrency Assets. For one, they transferred part of the Stolen Cryptocurrency Assets to custodial wallets owned by CEXs.[30] This made their identification somewhat inevitable. Because of the volume and nature of the transactions they send and receive, custodial wallets are easily identifiable on the blockchain. Further, as CEXs are

[24] *CLM v CLN* [2022] SGHC 46 at [61]-[64].
[25] *CLM v CLN* [2022] SGHC 46 at [61]-[64].
[26] *CLM v CLN* [2022] SGHC 46 at [83].
[27] Low, D. (20 May, 2022). *Singapore High Court blocks potential sale and transfer of rare NFT.* The Straits Times.
[28] See Section II(4).
[29] *CLM v CLN* [2022] SGHC 46 at [46].
[30] *CLM v CLN* [2022] SGHC 46 at [21].

incorporated entities, they are typically under obligations to prevent money laundering, which they fulfil by performing know-your-client and identity verification procedures on customers as a prerequisite for access to their services.[31] These procedures precipitated the ancillary disclosure orders in SUM 2444, which led to the Second and Third Defendants disclosing email addresses and documents identifying the Fourth and Fifth Defendants.[32]

28 Had the First Defendants done otherwise, things might have been different. While everything is public on the blockchain, the Stolen Cryptocurrency Assets could have sat in perpetuity in non-custodial wallets. If that were the case, there would have been no means of identifying the owners of those wallets.

29 Additionally, as Lee J astutely noted in *CLM*, it is easy to dissipate cryptocurrency assets such that they may be completely untraceable.[33] Although transactions are public on the blockchain, certain decentralised applications ("**dApps**"), such as tornado.cash on the Ethereum network, serve as private transaction protocols that obfuscate transactions by breaking the link between the sending address and receiving address, making transactions untraceable.[34] Unlike CEXs, these dApps are generally run by code and not actively managed by humans. There would therefore be no meaningful party to compel to disclose any information – even if disclosure orders were made against creators of such dApps, they would simply have no means to disclose anything even if they wanted to – the nature of dApps is such that they do not and cannot collect identification information. The Stolen Cryptocurrency Assets could also have been bridged to private blockchains[35] such as the Secret Network.[36]

30 In short, it is entirely plausible that the Stolen Cryptocurrency Assets could have vanished into the ether. Had the First Defendants done any of the above instead of sending the Stolen Cryptocurrency Assets to CEXs, any injunction would have been an academic exercise of cold comfort to the Plaintiff. No disclosure order would have been possible.

31 The subject-matter of the High Court's subsequent injunction to stop the sale and transfer of BAYC#2162 also made such an injunction more appropriate. The reason for this is obvious – BAYC#2162 is a unique token within a collection that consists of only 10,000 tokens.[37] There will only ever be one token answering to its description.

[31] George, B. (26 March, 2022). What Is KYC and Why Does It Matter For Crypto? Retrieved from CoinDesk: https://www.coindesk.com/learn/what-is-kyc-and-why-does-it-matter-for-crypto/.
[32] *CLM v CLN* [2022] SGHC 46 at [79]-[81].
[33] *CLM v CLN* [2022] SGHC 46 at [54].
[34] afeyda. (April, 2022). *Introduction to Tornado Cash*. Retrieved from tornado.cash: https://docs.tornado.cash/general/readme.
[35] In contrast with public blockchains such as the Bitcoin and Ethereum Network.
[36] johnniecosmos. (30 November, 2020). *Ethereum Bridge*. Retrieved from Github: https://github.com/scrtlabs/EthereumBridge/blob/master/README.md.
[37] Low, D. (20 May, 2022). *Singapore High Court blocks potential sale and transfer of rare NFT*. The Straits Times.

Therefore, laundering it through private transaction protocols would be futile – unlike fungible tokens like ETH, any wallet that receives BAYC#2162 would be identifiable *ipso facto*. The non-fungible nature of NFTs also allows third-parties to easily identify and isolate NFTs subject to injunctions. Popular decentralised NFT marketplace OpenSea has already disabled trading of BAYC#2162 in compliance with the injunction.[38]

IV. Conclusion

32 Cryptocurrency is not a monolith – the sheer possibilities are manifold, limited only by the creativity and innovation of those in the space. On the one hand, the identification of the Fourth and Fifth Defendants via the tracing of the Stolen Cryptocurrency Assets into the custodial wallets of the Second and Third Defendants is something unique to cryptocurrencies – it would not have been possible but for the transparent nature of blockchains. On the other hand, it is not for no reason that crypto has attracted so many bad actors. For every one instance where injunctive reliefs are appropriate, there are perhaps dozens where they would be futile.

33 In recent years, new developments have shone some light into the murky waters of non-custodial wallets. One such development is the Travel Rule, adopted by the Monetary Authority of Singapore in late-2019 on the recommendation of the global Financial Action Task Force. The Travel Rule requires that transactions incoming to and outgoing from payment service providers (such as CEXs) include the name of the originator or beneficiary.[39] However, such developments are ultimately effective only to some extent – as discussed above, it is possible to break a chain of transactions with private transaction protocols.

34 While *some* regulation is inevitable and perhaps should be welcomed, any expectation that the world of crypto will eventually be fully regulated or that the courts will one day be fully equipped to deal with any crypto-related situation should perhaps be tempered – crypto is an unruly beast that was meant to never be fully tamed or subjugated. Since the genesis of Bitcoin, it was built on tenets such as decentralisation, trust-lessness and the eradication of middlemen – aspects that are antithetical to and do not lend themselves readily to complete regulation and oversight.

[38] Avan-Nomayo, O. (20 May, 2022). OpenSea disables Bored Ape NFT amid legal case in Singapore. *The Block Crypto*. See also https://opensea.io/assets/ethereum/0xbc4ca0eda7647a8ab7c2061c2e118a18a936f13d/2162.
[39] Monetary Authority of Singapore. (5 December 2019). *MAS Notice PSN02 - Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Service Licence (Digital Payment Token Service)*, at [13].